

ACCEPTABLE USE POLICY

Enterprise Platform and AI Services

Effective Date: 07/21/2026

This Acceptable Use Policy (“AUP”) governs access to and use of the services provided by ai12z, Inc. (“ai12z”), including hosted software, APIs, web controls, copilots, digital assistants, search, GEO/AEO capabilities, connectors, tools, beta features, and related services (collectively, the “Services”). This AUP is incorporated into the applicable Master Subscription Agreement, Order Form, or other agreement between ai12z and the customer (“Customer”). Capitalized terms not defined here have the meanings given in the applicable agreement.

Customer is responsible for compliance with this AUP by its Affiliates, Authorized Users, administrators, contractors, end users, and anyone who accesses the Services through Customer’s accounts, applications, credentials, integrations, or deployments.

1. General Requirements

- 1.1 Customer may use the Services only for lawful, authorized purposes and in compliance with applicable laws, regulations, contractual obligations, Documentation, and this AUP.
- 1.2 Customer must provide accurate account information, protect credentials and API keys, apply reasonable access controls, and promptly notify ai12z of suspected compromise, unauthorized access, or misuse.
- 1.3 Customer must not encourage, assist, enable, or knowingly permit another person to engage in prohibited conduct through the Services.

2. Illegal, Fraudulent, or Harmful Activity

Customer may not use the Services to create, facilitate, promote, transmit, or support:

- activity that violates applicable law, court order, regulation, export control, sanction, or the legal rights of another person;
- fraud, scams, phishing, identity theft, credential theft, deceptive commercial practices, forged communications, or financial crime;
- credible threats, targeted harassment, stalking, extortion, coercion, or unlawful discrimination;
- terrorism, violent extremist activity, instructions to commit violent wrongdoing, or material support for unlawful violence;
- sexual exploitation or abuse of children, child sexual abuse material, grooming, or any sexual content involving minors;
- non-consensual intimate imagery, sexual exploitation, or unlawful pornographic content;
- the sale, distribution, or procurement of illegal drugs, illegal weapons, explosives, or other prohibited goods or services;
- content or conduct intended to encourage or facilitate imminent self-harm, suicide, or serious bodily injury; or
- any other activity that creates a material risk of harm to individuals, property, ai12z, the Services, or third parties.

3. Security, Abuse, and System Integrity

Customer may not, except to the extent expressly authorized in writing by ai12z:

- probe, scan, test, or exploit a vulnerability of the Services or related systems;
- bypass authentication, rate limits, subscription controls, safety features, access restrictions, usage limits, or technical protections;
- introduce malware, ransomware, viruses, worms, logic bombs, harmful code, malicious files, or unauthorized tracking technology;
- interfere with, disrupt, overload, degrade, or deny service to the Services or another customer;
- gain unauthorized access to accounts, systems, networks, models, prompts, Customer Content, or data;
- reverse engineer, decompile, disassemble, extract, reconstruct, discover, or attempt to discover source code, nonpublic prompts, model weights, system instructions, algorithms, or security mechanisms;
- use automated means to scrape, harvest, copy, or extract the Services, Documentation, or other customers’ information outside authorized interfaces;

- benchmark the Services for the purpose of developing or marketing a directly competing product without ai12z's prior written consent; or
- use multiple accounts, identities, organizations, or technical methods to evade enforcement or usage restrictions.

4. Privacy, Personal Data, and Sensitive Information

- 4.1** Customer must have a valid legal basis and all required notices, consents, permissions, and agreements before submitting, connecting, retrieving, or otherwise processing personal data through the Services.
- 4.2** Customer may not collect or process personal data through deception, unlawful surveillance, unauthorized profiling, or circumvention of privacy settings or consent controls.
- 4.3** Customer may not submit or process highly sensitive or regulated data—including protected health information, payment-card data, government-issued identification numbers, biometric identifiers, precise geolocation, authentication secrets, or information subject to heightened statutory protection—unless that data type and use are expressly authorized in the applicable Order Form or DPA and Customer uses the approved configuration and safeguards.
- 4.4** Customer must not expose confidential information, personal data, credentials, or sensitive Customer Content in public prompts, public demonstrations, public logs, or unsecured integrations.
- 4.5** Customer may not use the Services to identify an anonymous person, infer highly sensitive traits, or combine data sets in a manner prohibited by applicable law.

5. Intellectual Property and Content Rights

Customer may not use the Services to:

- infringe, misappropriate, or violate copyrights, trademarks, trade secrets, patents, database rights, publicity rights, privacy rights, or other rights;
- upload, crawl, connect, copy, transform, publish, or distribute content without sufficient authorization;
- remove or falsify copyright, attribution, source, provenance, watermark, or rights-management information;
- impersonate ai12z, another company, public official, professional, or individual in a deceptive or unlawful manner; or
- represent Output as verified, approved, authored, or endorsed by a person or organization when it is not.

6. AI-Specific Use and Human Oversight

- 6.1** Customer must evaluate Output for accuracy, appropriateness, bias, timeliness, completeness, and legal compliance before relying on, publishing, communicating, or acting on it.
- 6.2** Customer may not represent that Output is guaranteed to be accurate, complete, current, unbiased, non-infringing, or independently verified by ai12z.
- 6.3** Customer may not use Output as the sole basis for a decision that determines or materially affects a person's employment, education, housing, credit, lending, insurance, healthcare, legal rights, access to essential services, or other similarly significant opportunity or benefit. Such uses require qualified human review, appropriate testing, documented oversight, and compliance with applicable law.
- 6.4** Customer may not use the Services for automated social scoring, unlawful biometric categorization, unlawful emotion recognition, deceptive manipulation, exploitation of vulnerable individuals, or other prohibited or high-risk practices under applicable law.
- 6.5** Customer must not intentionally manipulate model behavior to defeat safety controls, generate prohibited content, conceal unlawful activity, or obtain restricted information.
- 6.6** The Services must not be used as an emergency service or as the only means of contacting police, fire, medical, crisis, security, or other emergency personnel. Customer must provide appropriate emergency and escalation instructions for deployments where urgent safety issues may arise.

7. Transparency, Communications, and End Users

- 7.1** Where the Services interact directly with individuals, Customer must clearly disclose that the individual is interacting with an artificial intelligence system unless the artificial nature of the interaction is otherwise obvious and no disclosure is required by applicable law.
- 7.2** Customer must not use the Services to create deceptive endorsements, fabricated reviews, misleading testimonials, false affiliations, undisclosed synthetic personas, or materially misleading representations.
- 7.3** Customer must provide end users with appropriate privacy notices, terms, consent mechanisms, escalation paths, and contact information for Customer's deployment.
- 7.4** Customer may not send spam, junk mail, chain letters, unsolicited bulk messages, or automated communications in violation of applicable marketing, telemarketing, or communications laws.
- 7.5** Customer must not use the Services to mislead an individual into believing the assistant is a licensed professional, human employee, government representative, or emergency responder when it is not.

8. Crawling, Connectors, APIs, and Third-Party Systems

- 8.1** Customer may direct the Services to crawl, retrieve, index, or connect to content only when Customer has authorization to access and process that content and the activity complies with applicable law, contractual restrictions, access controls, and website or system requirements.
- 8.2** Customer may not use the Services to bypass paywalls, authentication, robots or access controls, technical restrictions, or contractual limitations, unless Customer is authorized to do so by the owner or operator of the affected system.
- 8.3** Customer is responsible for data transmitted to or received from third-party systems, for configuring permissions and filters, and for ensuring that connectors do not retrieve data beyond Customer's authorization.
- 8.4** Customer may not use API keys, credentials, tokens, cookies, session data, or headers that Customer is not authorized to use or disclose.

9. Regulated and Specialized Uses

- 9.1** Customer must not use the Services in a regulated environment or for regulated data unless the applicable Order Form, DPA, and implementation configuration expressly support that use.
- 9.2** Customer is responsible for determining whether sector-specific requirements apply, including requirements relating to healthcare, financial services, education, employment, insurance, government, children, accessibility, records retention, consumer protection, and professional licensing.
- 9.3** Customer may not use the Services to make clinical diagnoses, prescribe treatment, provide emergency medical guidance, render legal opinions, execute financial trades, or provide individualized regulated professional advice without appropriately qualified professionals, required licenses, and legally sufficient oversight.
- 9.4** Customer may not knowingly direct the Services to children in violation of applicable child-protection or parental-consent requirements. Customer must obtain ai12z's prior written approval before deploying the Services primarily for children under the age threshold established by applicable law.

10. Enforcement

- 10.1** ai12z may investigate suspected violations and may require Customer to provide information reasonably necessary to evaluate compliance. ai12z may use automated and manual measures to detect abuse, security threats, service integrity issues, and violations of this AUP, consistent with the applicable agreement and law.
- 10.2** If ai12z reasonably believes a violation has occurred or is likely to cause harm, ai12z may remove or restrict access to affected content, credentials, users, features, integrations, or accounts; suspend affected Services; preserve information as legally required; or report unlawful conduct to appropriate authorities.

10.3 Where practicable and appropriate, ai12z will notify Customer and provide an opportunity to cure. ai12z may act immediately where necessary to address unlawful activity, a security threat, imminent harm, material service disruption, or legal requirements.

10.4 Repeated, intentional, or material violations may result in termination under the applicable agreement. Suspension or termination does not limit other remedies available to ai12z.

11. Reporting Concerns

Customer should promptly report suspected abuse, security vulnerabilities, unlawful content, compromised credentials, or other violations to compliance@ai12z.com. Security researchers must not conduct testing without prior written authorization from ai12z.

12. Changes to this AUP

ai12z may update this AUP to address new service features, threats, abuse patterns, laws, or regulatory requirements. Material changes will not apply retroactively and will not materially reduce Customer's rights during a current paid Subscription Term unless required by law or necessary to address an urgent security or safety risk. The effective date above will be updated when this AUP changes.